

**BOB FILNER, CALIFORNIA, CHAIRMAN**

CORRINE BROWN, FLORIDA  
 VIC SNYDER, ARKANSAS  
 MICHAEL H. MICHAUD, MAINE  
 STEPHANIE HERSETH SANDLIN, SOUTH DAKOTA  
 HARRY E. MITCHELL, ARIZONA  
 JOHN J. HALL, NEW YORK  
 DEBORAH L. HALVORSON, ILLINOIS  
 THOMAS S.P. PERRIELLO, VIRGINIA  
 HARRY TEAGUE, NEW MEXICO  
 CIRO D. RODRIGUEZ, TEXAS  
 JOE DONNELLY, INDIANA  
 JERRY McNERNEY, CALIFORNIA  
 ZACHARY T. SPACE, OHIO  
 TIMOTHY J. WALZ, MINNESOTA  
 JOHN H. ADLER, NEW JERSEY  
 ANN KIRKPATRICK, ARIZONA  
 GLENN C. NYE, VIRGINIA

MALCOM A. SHORTER  
 STAFF DIRECTOR

**U.S. House of Representatives****COMMITTEE ON VETERANS' AFFAIRS**

ONE HUNDRED ELEVENTH CONGRESS

335 CANNON HOUSE OFFICE BUILDING

WASHINGTON, DC 20515

<http://veterans.house.gov>**May 12, 2010****STEVE BUYER, INDIANA, RANKING**

CLIFF STEARNS, FLORIDA  
 JERRY MORAN, KANSAS  
 HENRY E. BROWN, JR., SOUTH CAROLINA  
 JEFF MILLER, FLORIDA  
 JOHN BOOZMAN, ARKANSAS  
 BRIAN P. BILBRAY, CALIFORNIA  
 DOUG LAMBORN, COLORADO  
 GUS M. BILIRAKIS, FLORIDA  
 VERN BUCHANAN, FLORIDA  
 DAVID P. ROE, TENNESSEE

KINGSTON E. SMITH  
 REPUBLICAN STAFF DIRECTOR  
 AND CHIEF COUNSEL

The Honorable Eric K. Shinseki  
 Secretary  
 U.S. Department of Veterans Affairs  
 810 Vermont Avenue, NW  
 Washington, DC 20140

Dear Mr. Secretary,

I am writing you with great concern about VA's continuing material weakness in protecting veterans' personal information from data breaches. The Department of Veterans Affairs has informed the Committee on two data breach incidents in Texas in the last two weeks. In May 2006, the VA suffered the largest data breach in federal government, as well as the second largest data breach in American history. The May 3, 2006 theft of a personally owned laptop belonging to a VA employee, containing the sensitive personal data of 26.5 million veterans and 2.2 million guard and reserve component service members and families, cost the VA over \$28 million in notification procedures and an additional \$20 million class action suit.

During the 109<sup>th</sup> Congress, the Department opposed my legislation, H.R. 5835, amended, the Veterans Identity and Credit Security Act of 2006, which passed the House by a vote of 408-0. The Department argued that the legislation was not necessary, and VA could internally remedy and correct the deficiencies and vulnerabilities that allowed this massive breach to occur. The language of H.R. 5835 was incorporated into Public Law 109-461.

It was hoped that Public Law 109-461 would provide the VA with the necessary tools with which to combat information security flaws within the VA's IT infrastructure. Title IX, Subchapter II, §5722 (b)(5) requires annual security awareness training for all Department employees, contractors, and all other users of VA sensitive data and Department information systems. That training must identify the information security risks associated with the activities of such employees, contractors, and users and their responsibilities to comply with Department policies and procedures designed to reduce such risks.

On August 4, 2006, VA issued VA Directive 6500, which details the steps by which the Department would provide compliance with system security measures, and on September 18, 2007, the Department issued the National Rules of Behavior for employees and contractors to use as a means to secure the data contained in VA's information systems. Upon further investigation, we learned that in November 2009, the Department had issued an additional directive for VA to incorporate VA Acquisition Regulation 852.273-75 into all contracts where this type of information might be accessed.

Even with these measures in place, on April 28, 2010, the Committee was notified of a stolen unencrypted laptop which had access to VA medical center data, including the personal identifying information of approximately 644 veterans. It is apparent to me that the details of

these breaches clearly indicate the VA lacks focus on its primary responsibility of protecting veterans' personal information. It also shows that senior managers have neglected their responsibilities, that there is no clear definition of responsibilities; nor a delineation of responsibilities. In short, there is a preponderance of evidence of a severely dysfunctional and broken procurement process in the Veterans Health Administration.

I applaud your actions in February 2009 to order the review of 22,729 contracts for missing information security clauses. This review took seven months and indicated that 6,440 contracts did not have the required the information security clause. Of these contracts 5,665 had the clause added, and 578 contractors refused to sign the clause. An additional 197 contracts still required the clause as of November 2009. Most troubling is the fact that 578 contractors refused to modify and sign the clause, without any apparent VA action to enforce its IT security policies. I have requested the VA General Counsel opinions regarding the status of these contractors or if the department has any obligation under the Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 111-5, Title XIII) to issue a public announcement of the data breach.

The most current breach involved a service disabled veteran owned business that had an unencrypted company laptop stolen. This company has 69 separately negotiated contracts with 13 VISNs. A review of these contracts indicates that 25 of the contracts did not include an information security clause. I can only conclude from this incident that VA's procurement processes seriously lack standardization in content, failure to articulate requirements, and an absence of compliance oversight.

I am still waiting to discuss with your staff my procurement reform legislation (H.R. 4221) which I provided to the department last December. I sincerely believe this legislation would provide the department with resources and legal tools to address and remedy these serious deficiencies.

With all these measures to protect our nation's veterans' information, it begs the question of why unencrypted devices are still accessing the VA's networks and storing information locally. We would like to express our deepest concern about the continued use of unencrypted devices within VA, despite the ongoing efforts to stop such use. Please advise the Committee within the next 30 days of your plan to decrease and eventually eliminate the use of unencrypted devices within the VA, particularly in the health care business line.

We look forward to any information you can provide in this regard. If you have any questions, please contact Arthur Wu, Staff Director for the Subcommittee on Oversight and Investigations at (202) 225-3527.

Sincerely,

A handwritten signature in dark ink, appearing to read "Steve Buyer", with a stylized flourish extending from the end.

Steve Buyer  
Ranking Republican Member

SB:dwc